

CONFIDENTIAL

NCSC-4



**NATIONAL POLICY
ON
CONTROL OF COMPROMISING EMANATIONS (U)**

*NATIONAL COMMUNICATIONS
SECURITY COMMITTEE*

NSA review completed

The Compilation of Information Contained
Herein is Classified CONFIDENTIAL.

Classified by the NCSC.
Review January 16, 2001.

CONFIDENTIAL

CONFIDENTIAL

NCSC

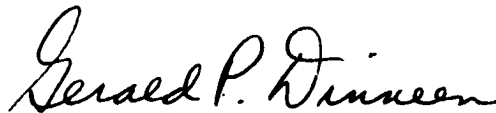
NATIONAL
COMMUNICATIONS
SECURITY
COMMITTEE

FOREWORD

(U) The National Policy on Control of Compromising Emanations (U) has been revised to place more emphasis on emanations security, to insure that TEMPEST requirements are considered in the procurement of new systems and equipment, and to place more emphasis on promoting TEMPEST awareness, under the proper security controls, within private industry.

(U) This policy supersedes the National Policy on Control of Compromising Emanations, dated 1 June 1976.

FOR THE EXECUTIVE AGENT FOR COMMUNICATIONS SECURITY:



Gerald P. Dinneen
Chairman

CONFIDENTIAL

CONFIDENTIAL

**NATIONAL POLICY
ON
CONTROL OF COMPROMISING EMANATIONS (U)**

16 January 1981

Section I—Policy

1. It is the policy of the U.S. Government to prevent the loss of national security information (Government-derived classified information or Government-derived unclassified information relating to national security) through compromising emanations. The decision on applications involving unclassified information relating to national security will be made on a case-by-case basis.

Section II—Background

2. Equipment used for information processing may emit signals that are compromising. Laboratory and field tests have established that such compromising signals can be propagated through space and along nearby conductors. The interceptability, propagation ranges, and analysis of such emanations are affected by a variety of factors, e.g., the functional design of the information-processing equipment, its installation, and environmental conditions related to physical security and ambient noise. Therefore, the measures required to protect classified information and unclassified information relating to national security are variable and involve the selective application of available protective means. Such protective measures require periodic re-evaluation to determine their continued effectiveness. Measures to control compromising emanations are categorized under the broad heading of emission security, which is defined as follows:

Emission Security—That component of communications security (COMSEC) which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

Section III—Purpose and Scope

3. All equipment used to process national security information or unclassified information relating to national security is subject to the provisions of this policy. Compromising emanations are defined as unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the national security information transmitted, received, handled, or otherwise processed by any information-processing equipment. This policy is binding on all departments, and agencies, of the Federal Government which handle national security information. In this document, the term

The Compilation of Information Contained Herein is Classified **CONFIDENTIAL**.

CONFIDENTIAL

CONFIDENTIAL

"Organization" is used to cover those Federal Government departments and agencies which handle national security information. Classified information is defined in Executive Order 12065.

Section IV—Guidelines

4. The following guidelines shall be used in complying with the intent of this policy:

a. National technical criteria shall be developed by the SCOCE and published in the National COMSEC Issuance System.

b. Based upon threat and vulnerability assessment information, organizations shall select the appropriate emission security methods to protect their information processing equipment, systems, and facilities. The protection afforded the equipment, systems, and facilities must meet the standards set forth in the National COMSEC Issuance System.

c. In the interests of long-range economy and standardization, the objective in the procurement of new equipments is to obtain operationally suitable equipment which has been designed to meet the compromising emanations standards defined in the National COMSEC Issuance System.

d. To obtain maximum effectiveness by the most economical means in the various compromising emanations security programs affected by this policy, Organizations shall exchange technical information freely, coordinate programs, and participate in consolidated programs, such as training, wherever possible.

Section V—Responsibilities

5. In accordance with provisions of the National Communications Security Directive dated 20 June 1979:

a. The National Communications Security Committee (NCSC) has established a Subcommittee on Compromising Emanations (SCOCE) to provide the forum for exchange of information on compromising emanations among the U.S. Government departments and agencies concerned with the problem. SCOCE's responsibilities are contained in the NCSC Directive on the Subcommittee on Compromising Emanations (U), dated 15 April 1980.

b. Heads of all Organizations are responsible within their organizations for:

(1) Planning, programming, and funding for, implementing and managing compromising emanations control programs to implement the provisions of this policy and the National COMSEC Issuances on compromising emanations. The programs should include provisions for:

(a) Establishing compromising emanations control measures during research, development, test and evaluations (RDT&E) and procurement of new information-processing equipment and systems.

(b) Conducting RDT&E as necessary to improve methods for controlling compromising emanations.

(c) Evaluating and testing for compromising emanations from existing

CONFIDENTIAL

CONFIDENTIAL

equipment, systems and facilities in order to develop a priority schedule, based on threat and vulnerability assessments, for taking corrective measures.

(d) Taking corrective measures as required to control compromising emanations from existing equipment, systems, and facilities.

(e) Requiring that contractors under their cognizance comply with this policy.

(2) Promulgating directives, standards, and instructions to implement the provisions of this policy and the National COMSEC Issuances on compromising emanations, within their Organizations.

(3) Coordinating their programs through the SCOCE to obtain mutual support and to avoid duplication of effort.

(4) Providing copies of reports containing equipment test results and studies of techniques to the SCOCE TEMPEST Information Center.

(5) Providing information, subject to the applicable security controls, on the control of compromising emanations to U.S. industry for contractual development or procurement of equipment and systems which will be used to process national security information.

c. The Director, National Security Agency, in addition to those responsibilities listed in paragraph 5b, is responsible for:

(1) Performing technical analysis to determine the degree to which compromising emanations affect cryptographic principles, techniques, and equipment.

(2) Approving the application of compromising emanations suppression techniques and protective measures to cryptographic techniques and equipment and certifying the TEMPEST acceptability of cryptographic equipment.

(3) Initiating research and development projects on techniques, protective measures, and standards for controlling compromising emanations from cryptographic equipment.

(4) Providing consultation, advisory information, and planning assistance to other Organizations.

(5) Providing guidance to Organizations on the security classification and control of information pertaining to compromising emanations to include guidance on the releasability of such information to contractors and foreign nations.

(6) Operating for SCOCE a national TEMPEST Information Center which provides for a continuing exchange of compromising emanations information among U.S. Government organizations.

(7) Conducting the Industrial TEMPEST Program under SCOCE cognizance to encourage U.S. industry to voluntarily develop and offer to the U.S. Government equipment and systems which have been designed to minimize compromising emanations.

CONFIDENTIAL**3**

CONFIDENTIAL

CONFIDENTIAL